ORIGINAL

Before the
Federal Communications Commission
Washington, D.C. 20554

RECEIVED
DEC 14 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

To: The Commission

COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.

AIRTOUCH COMMUNICATIONS, INC.

Pamela J. Riley
David G. Gross
AirTouch Communications, Inc.
1818 N Street, N.W., Suite 800
Washington, D.C. 20036
(202) 293-3800

Michael W. Mowery
AirTouch Communications, Inc.
2999 Oak Road, MS1025
Walnut Creek, CA 95596
(510) 210-3804

No. of Copies rec'd 0+4
List ABCDE

December 14, 1998

SUMMARY

AirTouch supports Commission approval of the industry-developed standard for the CALEA compliance "safe harbor," J-STD-025, but opposes the addition of the so-called "punch list" items advocated by the FBI. None of the punch list items meets the standards established in Section 107 of CALEA.

Congress enacted CALEA to preserve the existing wiretapping ability of law enforcement agencies, not expand it, in the face of digital and wireless technologies. Accordingly, Congress intended the assistance capabilities in the statute to be narrowly construed. This is particularly appropriate, given that the statute specifically denies law enforcement agencies the right to dictate the "specific design" to be employed for telecommunications "equipment, facilities, services, features, or system configurations." The Commission should not facilitate an end run around this express limitation on law enforcement by requiring compliance with the FBI's design standards.

Section 107 of CALEA permits the Commission to adopt CALEA requirements only if the industry standard is deficient, and any requirement it adopts must (1) be a cost-effective method of meeting the Section 103 capability requirements, (2) protect privacy, (3) minimize cost to residential ratepayers, and (4) encourage new technologies and services. Also, the Commission must provide a reasonable time for compliance. In reaching its decision, the Commission is obligated to conduct its proceedings in an open, public, and accountable manner. To satisfy Section 107, the Commission must have evidence in the record to support its conclusions.

AirTouch must rely on its vendors for cost information, and it is difficult for vendors to provide reasoned estimates of the cost of compliance, given the vague and indeterminate nature of the punch list. The FBI has not helped narrow these proposed requirements down. As a result, there is currently no solid information on the cost of compliance in the record. Without such data, the Commission cannot make the necessary determination that the punch list requirements would be a cost effective way to achieve CALEA compliance. Conclusory determinations, in this regard, will not withstand scrutiny on appeal.

The punch list items do not meet the statutory criteria. At a minimum, the punch list items are not cost-effective. Given the ill-defined nature of the punch list and the resulting lack of precision in any cost estimates, it appears that the software-only costs for compliance with the punch list as a whole will be several hundred thousand dollars per switch, or hundreds of millions of dollars nationwide. Significant hardware costs will also be required. AirTouch also shows that specific punch list items fail to meet the statutory criteria:

Content of Subject-Initiated Conference Calls. The industry standard already provides for interception of conference call content to which the subject is a party; this punch list item would provide for interception of portions to which the subject is not a party, an extension of preexisting wiretap authority. Interception of the content of subject-initiated wireless conference calls should be limited to the content transmitted over the wireless link. This punch list item would require multiple call content channels for every conference call intercepted, multiplying the cost of such intercepts, and cannot be considered cost-effective.

Party Hold, Join, Drop on Conference Calls. This punch list item fails to meet the statutory criteria for similar reasons. In addition, it would be very complex and costly to implement and would not provide call-identifying information, as the Commission tentatively claims.

Subject-Initiated Dialing and Signaling Information. This, too, would expand law enforcement's wiretapping ability, and the information gathered does not constitute call-identifying information. The cost is difficult to estimate because of its indeterminate scope, but it will be substantial. It is not a cost-effective means of meeting CALEA's assistance requirements.

In-Band and Out-of-Band Signaling. The proposed notification messages do not constitute call-identifying information or call content and thus represents an expansion of law enforcement's interception capability and exceeds the specific requirements of Section 103. Providing such messages could be very complex and costly, given the wide variety of out-of-band signaling messages routinely generated by the operation of a wireless system. This would not be cost-effective.

Timing Information. The proposed timestamp requirement represents an attempt to dictate CMRS system design and configuration, in violation of Section 103. This is not part of a call, nor does it comport with the statutory definition of call-identifying information; it is not, therefore, a cost-effective method of complying with the assistance requirement. The detailed timestamp and delivery time requirements also go well beyond the requirements of Section 103 with respect to when call-identifying information must be transmitted.

Surveillance Status, Continuity Check Tone, Feature Status. AirTouch agrees with the Commission that these items constitute neither call content nor call-identifying information and are not, therefore, an assistance capability required by Section 103.

Dialed Digit Extraction. This proposed requirement would impose a very substantial cost on wireless carriers, which do not currently have any reason to detect and extract post-cut-through dialed digits. One vendor called this item "cost prohibitive." It is also unnecessary, since a call content channel will deliver the digits to law enforcement with a Title III intercept order. The post-cut-through digits are not call-identifying information, but content as far as the carrier is concerned. This proposal is not a cost-effective way of meeting an assistance capability set forth in Section 103. Moreover, providing all dialed digits as call-identifying information would fail to protect the privacy and security of digits used for purposes other than call routing, in violation of Section 107.

The Commission should endorse the industry J-STD-025, subject to the clarification proposed for location information, and should defer the difficult issues concerning packet-mode data to a further proceeding. Finally, the Commission should acknowledge that the June 30, 2000 compliance date for J-STD-025 will likely require extension, based on vendors' representations.

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

To: The Commission

COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.

AirTouch Communications, Inc. ("AirTouch"), by its attorneys, hereby submits its comments in response to the Commission's *Further Notice of Proposed Rulemaking,* FCC 98-282 (Nov. 5, 1998) ("*FNPRM*") in this proceeding. AirTouch supports Commission approval of the industry-developed J-STD-025 as a "safe harbor" for carrier compliance with the requirements of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"),[1] but opposes the imposition of new requirements based on the FBI-Department of Justice so-called "punch list," as the *FNPRM* proposes.

AirTouch is filing comments with as much detail concerning the punch list items as it can. Carriers, however, are almost wholly dependent on their vendors for information concerning the feasibility and cost of implementing the design changes that the punch list entails. For that reason, AirTouch wrote a letter to each of its four vendors (Ericsson, Lucent, Motorola, and Nortel) shortly after issuance of the *FNPRM* seeking detailed information for use in filing its comments. (A copy of a representative letter is attached as Attachment A.) The vendors have responded to varying

---

[1] Pub. L. No. 103-414, 108 Stat. 4279 (1994).

degrees, but all are vague and indeterminate on many points. All four vendors have stated that it is difficult to estimate the cost of punch list compliance with reasonable certitude because of the fact that the punch list has not been "nailed down" with sufficient precision. Despite the industry's efforts to develop tentative standards for the punch list items through the TR45.2 Enhanced Surveillance Standard ("ESS") process, the FBI has failed to assist in the Committee's attempt to narrow the technical issues. Instead of providing more precise definitions of what it sought under the punch list, the FBI has kept the items vague, broadly-worded, and all-inclusive, and has frustrated the standards process. As a result, the punch list remains an elusive target for commenters. In light of the lack of solid information regarding the cost and feasibility of implementing the punch list items, the Commission clearly cannot make the required statutory determination that punch list compliance is a "cost effective" way of achieving compliance with CALEA.

I. ANY CALEA ASSISTANCE REQUIREMENTS THE COMMISSION IMPOSES MUST NARROWLY MEET THE STATUTORY CRITERIA, BASED ON A FACTUAL RECORD, TO WITHSTAND JUDICIAL REVIEW

A. Congress Intended CALEA's Assistance Requirements to Be Construed Narrowly for the Preservation of Existing Wiretap Capability, Not as a Broad Charter for New Capabilities

Congress enacted CALEA in 1994 in response to concerns expressed by law enforcement officials that the introduction of new technologies into the nation's telecommunications network posed a threat to their continued ability to engage in lawfully authorized wiretapping or eavesdropping activities. The acknowledged purpose of this law, Congress said, was to "preserve" law enforcement's ability to engage in lawfully authorized interceptions in a digital and wireless age,[2] not to grant law enforcement agencies a "wish list" of unlimited new electronic surveillance powers.

---

[2] H.R. Rep. No. 103-827, at 9 (1994) ("House Report").

Congress simply sought to give law enforcement agencies the ability to engage in the same sorts of authorized electronic surveillance that were already in use, despite the introduction of new technologies and services, at the same time balancing the objectives of protecting privacy and encouraging the use of new technologies.[3] Accordingly, in describing the assistance capability requirements that Section 103 imposes on carriers, Congress emphasized that it did "not intend[] to guarantee 'one-stop shopping' for law enforcement" and that the legislation did "not purport to dictate" the "design of the service or feature at issue."[4] In addition, when it required carriers to provide only "reasonably available" call identifying information,[5] Congress emphasized that "if such information is not reasonably available, the carrier does not have to modify its system to make it available."[6] The capability requirements were narrowly defined and not intended to grant law enforcement the ability to engage in new forms of electronic surveillance:

> The Committee intends the assistance requirements in [Section 103(a)] to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. . . . The Committee expects industry, law enforcement, and the FCC to narrowly interpret the requirements.[7]

In other words, neither the FCC or law enforcement agencies were authorized to require any more than what Section 103 specifically requires. As a result, the FCC does not have the authority to "flesh out" Section 103(a) in response to a deficiency petition with supplementary rules going beyond the plain meaning of the assistance requirements in that section, and any such expansive

---

3 House Report at 13.

4 *Id.* at 22.

5 CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2); House Report at 22.

6 House Report at 22.

7 *Id.* at 22.

rules will be vulnerable on appeal and will not be entitled to *Chevron* deference by a reviewing court.[8] Instead, FCC-imposed requirements going beyond the industry standard must be rooted in the express requirements of Section 103(a).

B. A Narrow Interpretation Is Also Necessary to Prevent an FBI End Run around CALEA's Bar on Law Enforcement Dictation How Equipment and Networks Must Be Designed

An additional reason for a narrow interpretation of Section 103(a), in considering the FBI's punch list items, is that the statute specifically provides that it does not authorize law enforcement agencies or officers "to require any specific design of equipment, facilities, services, features, or system configurations."[9] The FBI has already attempted to persuade the telecommunications industry to include the punch list design features in the J-STD-025, and has failed. The punch list items, if mandatory, clearly would "require" a "specific design" of telecommunications networks. The statute does not permit the FBI to impose such requirements on carriers or manufacturers. Additionally, the capabilities contained in the punch list can be incorporated in FCC rules only if they are specifically necessary for achieving compliance with the express terms of Section 103(a), construed narrowly. The Commission should not — and by law cannot — permit its processes to be used by the FBI as a way around the express limitation in the statute on law enforcement dictation of design features.

C. Section 107(b) of CALEA Establishes Strict Criteria for Imposing Requirements Beyond the Industry Standard

CALEA "defers, in the first instance, to industry standards organizations" for implementation.[10] Accordingly, the "safe harbor" provision, Section 107(a), allows the establishment of standards by industry groups, after consultation with law enforcement agencies, and provides that

---

8 *See Chevron U.S.A. Inc. v. NRDC,* 467 U.S. 837, 842 (1984).

9 CALEA § 103(b)(1)(A), 47 U.S.C. § 1002(b)(1)(A).

10 House Report at 26.

a carrier or manufacturer shall be deemed in compliance with Section 103 "if it is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization" or by the FCC.[11]

Section 107(b) authorizes the Commission to promulgate rules, technical requirements, or standards, only if there are no industry standards or if the industry standards are shown to be deficient in response to a petition. Any such FCC-promulgated requirements must:

> (1) meet the assistance capability requirements of section 103 by cost-effective methods;
>
> (2) protect the privacy and security of communications not authorized to be intercepted;
>
> (3) minimize the cost of such compliance on residential ratepayers;
>
> (4) serve the policy of the United States to encourage the provision of new technologies and service to the public; and
>
> (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers during any transition period.[12]

The telecommunications industry responded to Section 107(a) of CALEA by working on a standard for broadband CMRS compliance with Section 103's capability requirements. The standard emerging from this process, J-STD-025, was adopted after extensive consultation with the FBI and other law enforcement agencies. Not satisfied, the FBI sought to incorporate an extensive "punch list" of additional design features into the industry standard. In many respects, this punch list lacked sufficient specificity to be incorporated into the standard, and the features sought by the FBI varied considerably over time, as well. In addition, some of the features the FBI sought were either too

---

11 CALEA § 107(a)(2), 47 U.S.C. § 1006(a)(2); *see* House Report at 26.

12 CALEA § 107(b), 47 U.S.C. § 1006(b); House Report at 27.

expensive or difficult to achieve reasonably, or otherwise did not conform to the statutory requirements. As a result, while J-STD-025 includes many provisions designed to meet the expressed needs of law enforcement agencies, including the FBI, the punch list was not incorporated into it. It is that punch list that is the principal subject of the *FNPRM* and these comments.

The Commission may adopt the punch list items, however, only if they satisfy the five criteria in Section 107(b). If the record does not demonstrate that the Commission has satisfied these criteria, its decision will be subject to reversal by a reviewing court. Accordingly, AirTouch will briefly address these criteria before turning to the punch list. As discussed herein, the punch list items do not satisfy the statutory criteria and should be rejected by the Commission.

1. Meet Section 103 Assistance Capability Requirements by Cost-Effective Methods

The Commission must determine whether each punch list item is necessary for compliance with Section 103's express requirements. Because these punch list items were *not* incorporated into the industry standard after due consideration by the standard-setting body, the Commission must further establish, based on the material of record of this proceeding, that each item achieves a requirement of Section 103 by "cost-effective methods."[13] In other words, the Commission must be not only determine that a particular punch list item is needed to satisfy one or more of the Section 103 assistance capability requirements, it must further establish the cost of implementing the punch list item and weigh its efficacy against the cost. In the absence of evidence in the open record concerning the cost of implementing each specific punch list item, the Commission clearly cannot make such a determination.

The need for an open, public record, by which the Commission's efforts will be measured in a reviewing court is pointed out by the legislative history. Congress said that it was giving the

---

[13] CALEA § 107(b)(1), 47 U.S.C. § 1006(b)(1).

FCC the authority to promulgate requirements in order "to add openness and accountability to the process of finding solutions to intercept problems. Any FCC decision on a standard for compliance with [CALEA] must be made publicly."[14]

Despite the need for open, public processes, the Justice Department and FBI have been promoting its punch list, and the alleged $2 billion cost of CALEA implementation, based on highly suspect, nonpublic information. On December 4, 1998, a group of trade associations wrote to the Attorney General asking that the Justice Department provide a full public accounting of its estimate of the cost of CALEA implementation, including all of its pricing assumptions.[15] On December 10, 1998, the same organizations wrote the Attorney General concerning presentations made to the FCC and others concerning the industry's CALEA compliance and punch list capabilities based on a so-called "ESI Simulator" that is "wholly inaccurate and misleading."[16]

The use of nonpublic information by the FBI in its attempt to persuade the FCC of its position makes a mockery of the open public process that Congress required for CALEA implementation. The danger of relying on nonpublic presentations by the FBI is highlighted by the misleading nature of at least some of its nonpublic presentations to date — the inaccuracy of which came to light only after industry groups were finally permitted to see the presentation. The Commission should ensure that the record here has sufficient cost and other data to support its action herein. In the absence of such record data, it should seek the relevant information from those parties who uniquely possess it — vendors, the FBI, and the Department of Justice — and make it part of

---

14 House Report at 27.

15 Letter dated December 4, 1998 to the Honorable Janet Reno from the Cellular Telecommunications Industry Association, Personal Communications Industry Association, Telecommunications Industry Association, and United States Telephone Association.

16 Letter dated December 10, 1998 to the Honorable Janet Reno from the Cellular Telecommunications Industry Association, Personal Communications Industry Association, Telecommunications Industry Association, and United States Telephone Association.

the record, subject to comment by the public, before it adopts any punch list requirements. Again, the Commission must ensure that its decision is made on the basis of an open, public factual record. Its failure to do so will be grounds for judicial reversal or vacation of any rules it adopts.

2. Protect Privacy and Security of Communications Not Authorized to be Intercepted

The Commission must establish that each requirement that it promulgates "protect[s] the privacy and security of communications not authorized to be intercepted."[17] This is of particular importance with respect to requirements that carriers provide law enforcement with call identifying information, in response to an authorization that does not permit interception of call content. Any requirement pertaining to the provision of call identifying information must ensure that the carrier is not obligated to provide call content as well, in order to safeguard the privacy of communications not authorized to be intercepted. Where content and call identifying information are intermixed and cannot readily be separated by the carrier, the statute does not permit the Commission to require carriers to provide access to the intermixed content and call identifying information.

Under the wiretap laws, the carrier must determine what is call content and what is call-identifying information in order to determine what it must deliver to a law enforcement agency, unless the requesting agency has obtained the lawful authority to obtain both. The carrier cannot simply hand off call content to a law enforcement agency that has lawful authority only to intercept call-identifying information, hoping that the officers will sort out content and "cover their ears" at appropriate times. Providing intercepted content to law enforcement officers who have not obtained a Title III warrant is legally problematic and could potentially subject the carrier to criminal liability.

---

[17] CALEA § 107(b)(2), 47 U.S.C. § 1006(b)(2).

3. Minimize Cost of Compliance on Residential Ratepayers

The statutory requirement that the Commission minimize the cost of CALEA compliance that is imposed on residential ratepayers[18] is more directly relevant when the Commission is adopting regulations for landline telephone companies that are subject to rate regulation than CMRS carriers that are not rate regulated. Nevertheless, the unreimbursed costs imposed on CMRS carriers to comply with CALEA will, in the end, affect the prices that subscribers, including residential subscribers, pay for service. Accordingly, when the Commission is considering whether to impose punch list design features on CMRS manufacturers and carriers, it is obligated to minimize the costs that will thereby be imposed on carriers and, ultimately, on subscribers. In the absence of sufficient cost data, the Commission plainly cannot satisfy this statutory determination — and requirement.

4. Encourage Provision of New Technologies and Services

In evaluating the punch list items, the agency must also serve the national policy of "encourag[ing] the provision of new technologies and services to the public."[19] This requirement's principal effect, in the current context, is that the Commission must consider whether a carrier considering the provision of a particular new technology or service may be discouraged from doing so because of the complexity or cost of complying with the punch list items that pertain to that new technology or service. In other words, the statute makes clear that the Commission may not impose burdensome or costly requirements on carriers' offerings of new technologies and services simply in order to satisfy the needs of law enforcement.

---

18 CALEA § 107(b)(3), 47 U.S.C. § 1006(b)(3).

19 CALEA § 107(b)(4), 47 U.S.C. § 1006(b)(4).

5. Provide a Reasonable Time and Conditions for Compliance

The Commission must also "provide a reasonable time and conditions for compliance."[20] AirTouch submits that this requires the Commission to establish a schedule for compliance that is flexible and provides sufficient time for (a) the development and adoption of any necessary industry standards in accordance with the generally accepted procedures for such standard-setting; (b) the development, design, and production by vendors of any changes to hardware and software needed for compliance with such new standards, once set, in the course of a normal product development and upgrade cycle; and (c) the implementation and deployment of such changes, once made generally available by vendors, in the normal course of business by carriers.[21]

D. To Withstand Judicial Review, the Commission Must Have a Factual Record Demonstrating Compliance with these Criteria

In the *Cincinnati Bell* case, the Court of Appeals held that when the FCC imposes regulatory restrictions on companies, it must have a record-based economic justification for the rules.[22] Rules based on the Commission's "broadly stated fears," or "predictive judgments" not supported by the record, were found to be arbitrary and capricious, even if the rules are adopted to further a "permissible goal under the Communications Act."[23] In that case, the Court concluded that the FCC's rulemaking was arbitrary because it lacked any "factual predicate."[24] The Court emphasized that the FCC must "supply a reasoned basis explaining why it chose to adopt a certain rule or rules[,] . . . and support for the agency's action must exist in the rulemaking record."[25] Moreover, the Court

---

20 CALEA § 107(b)(5), 47 U.S.C. § 1006(b)(5).

21 *See* Sections II.J and III.A, below, concerning the timing of implementation.

22 *Cincinnati Bell Telephone Company v. FCC,* 69 F.3d 752 (6th Cir. 1995).

23 *Id.* at 760, 763-64.

24 *Id.* at 767.

25 *Id.* at 763.

held that the FCC is "required to give an explanation when it declines to adopt less restrictive measures in promulgating its rules. . . . [C]onclusory statements[] . . . wholly fail to provide a reasoned explanation as to why the less restrictive alternatives . . . are insufficient."[26] Accordingly, the Commission must explain its rationale, based on the record, sufficiently for a reviewing court to determine how it reached its decision.[27]

This is especially true when the FCC bases its decision on cost-effectiveness, as it must here. It is well established that any analysis of costs and benefits requires, at the outset, that all benefits and costs, whether tangible or intangible, direct or indirect, be identified.[28] In the absence of such information, the resulting "analysis" cannot form the basis for a rule.[29] Accordingly, the Commission must be able here to point to detailed, specific cost information in the record of its rulemaking in order to sustain any decision to adopt any of the punch list items as CALEA requirements.

II. THE RECORD DOES NOT SUPPORT REQUIRING COMPLIANCE WITH THE DOJ-FBI "PUNCH LIST" ITEMS

To start, the FBI's so-called "punch list" of capabilities is misnamed. The capabilities not included in J-STD-025 do not represent uncompleted items on which there is agreement, like a contractor's punch list of items to be completed before final payment is made. Instead, it represents a law enforcement "wish list" — a demand for all the interception-related capabilities the FBI would like to have available to it. The capabilities in the punch list represent a substantial expansion of wiretap capability beyond the *status quo,* contrary to the express intention of Congress to *preserve,*

---

[26] *Id.* at 761.

[27] *Simms v. NHTSA*, 45 F.3d 999, 1004-05 (6th Cir. 1995), *quoting Neighborhood TV Co. Inc. v. FCC*, 742 F.2d 629, 639 (D.C. Cir. 1984).

[28] *See Consumers Federation of America v. CPSC,* 990 F.2d 1298, 1309 (D.C. Cir. 1993).

[29] *See Gas Appliance Manufacturers Association v. DOE,* 998 F.2d 1041, 1047 (D.C. Cir. 1993); *see also Chemical Manufacturers Association v. EPA,* 28 F.3d 1259, 1265 (D.C. Cir. 1994); *see generally California v. FCC,* 39 F.3d 919 (9th Cir. 1994), *cert. denied,* 514 U.S. 1050 (1995).

not *expand,* the preexisting interception capabilities of law enforcement with the transition to new technologies. Moreover, the FBI's insistence on the punch list items after unsuccessfully attempting to persuade industry standards bodies to include them in J-STD-025 constitutes an attempt to evade Section 103(b)(1) of CALEA, which denies the FBI authority to "require any specific design" in telecommunications "equipment, facilities, services, features, or system configurations" for CALEA compliance.

As shown in the following sections, the punch list items do not satisfy the requirements of Section 107(b). Indeed, the *FNPRM* found that several punch list items while potentially helpful to law enforcement, do not fall into any of the Section 103(a) categories. Even as to the items that the Commission tentatively proposed to require, the statutory criteria are not satisfied.

The punch list items are not sufficiently well defined to be implemented. Congress intended CALEA's assistance requirements to be interpreted narrowly. Accordingly, any requirements that the Commission may impose in response to the punch list would have to be defined very narrowly, in explicit detail. Many punch list items are sufficiently open-ended that they are not yet even near the standards-writing stage. Manufacturers cannot design solutions that will comply with vague, general, all-inclusive punch list items.

The punch list items will also be costly to implement, even after they are better-defined. Some of these items will be far more difficult or expensive to implement than others, and the cost will ultimately depend on just what is and is not required. The Commission currently has no record basis on which to conclude that any of the punch list items will constitute "cost-effective methods" for meeting the assistance requirements of Section 103, assuming it is even able to conclude that any given item will in fact meet a requirement of Section 103.

The vendors who have provided information to AirTouch have only very tentatively estimated the cost of implementing the punch list items, because of the need for further clarification

and narrowing of the requirements. These estimates are difficult to compare, due to the differing architectures and technologies employed, and they are inherently "fuzzy" because of the lack of any agreement on the scope of the punch list items. With these significant caveats in mind, the *very rough* estimates provided by certain of AirTouch's vendors appear to fall somewhere in the range between $100,000 and $300,000 per typical switch — for software costs alone.[30] In one case, the punch list software upgrades would cost nearly twice as much as the J-STD-025 software upgrade. Hardware changes would entail substantial additional costs as well, largely due to the cost of equipment for enabling post-cut-through dialed digit extraction. At a minimum, the cost of fully deploying the punch list items would be hundreds of millions of dollars in addition to the cost of complying with J-STD-025. For the reasons discussed herein, these punch list items exceed CALEA's requirements and should not be required by the Commission.

A. Content of Subject-Initiated Conference Calls

The FBI's punch list seeks to require interception of all content of conference calls initiated by the subject by means of the facilities under surveillance, including the content of legs of the conference call that are not currently conferenced together, using functions such as hold, call waiting, or three-way calling. The *FNPRM* tentatively concludes that the provision of the content of such subject-initiated conference calls falls within the assistance capability requirements of

---

[30] AirTouch's vendors have specified that it must not disclose more specific cost data because of justifiable confidentiality concerns. AirTouch notes that the FBI has been given vendor-specific cost data by some, if not all, manufacturers. The FBI clearly should not be using this cost data selectively to support its position, but should be providing the Commission aggregate data that fairly represents the manufacturers' cost estimates. This does not appear to be the case, however, given the FBI's unsupported claims that deferring the grandfather date for CALEA will cost $2 billion. Accordingly, any cost data offered by the FBI must be viewed with suspicion, if it is not supported by solid data. Moreover, the Commission should recognize that cost data provided to the FBI by vendors are necessarily very tentative and preliminary, and may be based on incomplete, inaccurate, or inconsistent assumptions concerning the details of the punch list items. Again, this critical information should be made available to all as part of a public record of decisionmaking in order to sustain the actions taken.

Section 103, even when the subscriber who is the subject of the surveillance has dropped off the call, to the extent the system architecture continues to connect the remaining parties together through the subscriber's facilities.[31]

The content of a subject-initiated conference call can be considered under J-STD-025 as being subject to interception, as long as the subject subscriber is a party to the call. The question raised by the punch list item, thus, is whether Section 103 requires interception of the content of those portions of a conference call to which the subscriber is *not* a party. AirTouch submits that communications should not subject to interception when no communications path to the wireless subscriber's handset exists. CALEA was intended to *preserve preexisting wiretap authority, not expand it.* In the case of a wire telephone subscriber, a traditional wiretap would provide access to the content of a conference call being carried over a subject's local loop, but would not provide access to the content of a conference call not being carried over that local loop. To preserve this capability in the wireless context without expanding it, a carrier must provide access to a conference call being transmitted over a radio channel to the subscriber's handset, but any portion of the conference call not being transmitted over such a radio channel is not a call to which the subject can be considered a party and should not be subject to interception. Accordingly, for purposes of subject-initiated wireless conference calls, the "subscriber's equipment, facility, or service" that is subject to interception should be limited to a communications path being transmitted to the subscriber's handset over a radio link.[32]

---

[31] *FNPRM* at ¶ 78.

[32] Given this position, AirTouch agrees with the Commission's tentative conclusion that a separate conversation, not linked to the conference call, between a conference participant other than the subject subscriber and another person would not be subject to interception when the separate conversation is placed on alternative facilities.

To reach any other conclusion would require that talk-paths through the switch that are *not* currently connected to the subscriber be considered part of the subscriber equipment. Not only would this result in an *expansion* of wiretapping authority, it imposes significantly greater costs. The carrier must have the capacity to intercept each leg of the conference call independently, instead of the single intercept needed to capture the content of the conference call while the subject is a party to it. Every time a conference call is initiated by a subject, call content channels would be needed for the maximum number of conference legs that could be sustained if the call were split, whether or not the subject ever left the call. These port and trunking costs multiply the cost of intercepting *every* conference call, even though the software cost of this feature may not be prohibitive. Thus, even if such a capability were considered an assistance requirement enumerated in Section 103, it still would not represent a cost-effective method for achieving compliance, and is therefore contrary to Section 107(b)(1). Moreover, the increased cost of such conference call interceptions may have an adverse effect on residential subscribers, contrary to Section 107(b)(3).

Whether this capability protects the privacy and security of communications that are not authorized to be intercepted, as required by Section 107(b)(2), depends on whether the particular Title III wiretap authorization for a given intercept covers the content of communications among parties other than the subject that are not transmitted to the subject's telephone. Requiring this capability would tend to discourage, rather than encourage, the provision of new services and technologies, contrary to Section 107(b)(4). This is because the added cost associated with conference call interception that this entails will give carriers a disincentive to provide expanded switch-based conference calling capabilities to their subscribers, and the resulting increased cost to the subscriber of placing conference calls through the carrier's switch may cause subscribers to seek an alternative source of conferencing, such as an external conference bridge.

B. Party Hold, Join, Drop on Conference Calls

The *FNPRM* tentatively proposes to require compliance with the punch list item concerning the real-time transmission, as call-identifying information, of the identity of parties to a conference call when they are placed on hold, join the call, or drop off the call.[33] AirTouch opposes this proposal.

This punch list item would also considerably expand the scope of electronic surveillance, instead of maintaining the *status quo*. Traditionally, call-identifying information was gathered by a pen register or a "trap and trace" facility that would display the pulses, audio tones, and other signaling messages outgoing or incoming over the subject's local loop. CALEA was intended to maintain the ability to capture and display the same type of information in a network utilizing digital or wireless technologies, not expand the scope of the information captured.[34] The information called for by this punch list item goes well beyond what Congress intended to be included in call-identifying information, because it is information that would traditionally not have been transmitted over the local loop and would not have been captured by a pen register or "trap and trace" facility, except to the limited extent that the mere fact that a party has joined or dropped a conference call is distinguished by a pulse or tone.

According to one vendor, the implementation of these capabilities "will be very complicated and difficult." Another vendor estimates the cost of the software modifications for identification of the parties coming on and off conference calls to be *twice* the cost of those needed to capture conference call content when split. Accordingly, this feature is neither needed to comply with Section 103 nor a cost-effective method of doing so, contrary to Sections 107(b)(1) and (b)(3).

---

33 *FNPRM* at ¶¶ 85-86.

34 *See* House Report at 21.

This punch list item may also discourage the implementation of sophisticated switch-based conference calling for the same reasons as discussed with the preceding item. Accordingly requiring this capability would contravene Section 107(b)(4).

C. Subject-Initiated Dialing and Signaling Information

The next punch list item the Commission tentative proposes to adopt as a requirement is a capability to provide to law enforcement, as call-identifying information, identification of a subject subscriber's use of services and features such as call forwarding, call waiting, etc.[35] AirTouch opposes this proposal.

In short, this punch list item would, contrary to Congressional intent, increase rather than preserve the interception capabilities of law enforcement. As with the foregoing punch list item, this capability does not generate call-identifying information because it does not constitute the kind of information that would have been captured and intercepted utilizing a pen register or "trap and trace" facility. At most, a pen register would have captured the transmission of tones, if tones were used for such services and features, but it would not have identified the effects of the transmission of those tones as resulting from the party's activation or deactivation of call forwarding. Moreover, the information that the FBI seeks does not even purport to "identify the origin, direction, destination, or termination" of a communication made or received by the subject subscriber, as the definition of call-identifying information requires.[36] The mere fact of enabling or disabling a feature such as call forwarding does not directly result in the forwarding of a call, and does not, therefore, yield call-identifying information.

Vendors were largely unable to provide estimates of the cost of implementing this feature because of its open-ended scope, potentially extending to any number of features. One vendor,

---

35 *FNPRM* at ¶¶ 91-93.

36 *See* CALEA § 102(2), 47 U.S.C. § 1001(2).

however, noted that implementing this feature would potentially require making changes to hundreds of existing services, because its switch architecture does not provide any generic mechanism for identification of feature invocation. Accordingly, substantial costs are expected for the development of the software needed to provide this facility, even if its scope were to be clarified. As a result, this item does not constitute a cost-effective method for meeting a Section 103 requirement and thus contravenes Section 107(b)(1) and, ultimately, Section 107(b)(3).

To the extent this capability would require providing law enforcement with information concerning feature changes that are entered remotely — *e.g.*, changes to a subject's cellular phone call forwarding feature status, when entered from another telephone — it clearly is not an interception of call identifying information concerning the subject's cellular telephone. No call would, in such a case, be placed to or from the subject's phone, and accordingly there would be no call about which to provide identifying information. Instead, the information would be provided concerning a call from another telephone entirely — one that is not the subject of an authorization for interception — and would provide a means of tracking the subject's whereabouts, rather than intercepting call-identifying information.[37] Congress clearly did not intend to authorize such open-ended, geographically unlimited surveillance by requiring the provision of call-identifying information. Accordingly, the provision of remotely entered dialed digits or features would violate the minimization requirement of Section 107(b)(2).

Obviously, if compliance with this punch list item is required and if clarification of its scope confirms its significant costs, carriers will have a significant disincentive to implement new features

---

[37] This assumes that the carrier's network was required to have the capability to capture information concerning the telephone (*e.g.*, telephone number) from which the feature change was remotely entered.

and facilities that will further increase their costs. As a result, requiring compliance with this punch list item would also be contrary to Section 107(b)(4).

D. In-Band and Out-of-Band Signaling

The Commission has tentatively proposed adoption of a punch list requirement to provide law enforcement, as either call-identifying information or call content, a notification message whenever any network message is sent to a subject subscriber's phone, such as ring, busy signal, call waiting, or message light.[38] AirTouch opposes this proposal.

First, such notification messages clearly do not constitute call-identification information because they do not identify the "origin, direction, destination, or termination" of a communication. Moreover, such notification messages would not have been generated by a pen register or a "trap and trace" facility. Accordingly, to require such notification messages as call-identification information would represent a major expansion of preexisting wiretapping authorization, not a preservation of the *status quo.*

In addition, the generation of such notification messages is not required by the statute if a Title III intercept is authorized. To the extent such network messages are conveyed as audible tones, the tones will be provided on a content channel in the same form that they are provided to the subject. CALEA does not require a carrier to create a "notification message" interpreting information already being provided over a content channel — in fact, Congress only intended that carriers provide intercepted information to law enforcement "in a format available to a the carrier"[39] — a standard that is fully satisfied when the audible network message (*e.g.,* ringing or busy signal) is provided on the audio content channel. Moreover, any requirement to provide out-of-band

---

[38] *FNPRM* at ¶¶ 95, 99.

[39] House Report at 22.

signaling information that is not represented by tones in the audible content channel would go well beyond the scope of a traditional landline wiretap.[40]

The cost and complexity of providing notification messages for such network events would be considerable, particularly if messages must be generated for a wide-ranging variety of out-of-band signaling messages. A cellular system generates out-of-band signaling messages almost constantly, including supervisory audio tones, control channel messages, and other signals that control the frequency, power, and other characteristics of a cellular call, not to mention the constant out-of-band supervisory data streams between the switch and the cell sites and between the various components of the cellular network, such as the switch, the HLR, and the VLR. These out-of-band network signaling messages are (in most cases) completely transparent to the user. If all such signaling transmissions had to be recorded and translated to messages for transmission to law enforcement authorities on a real-time basis, one vendor reports, "the difficulty . . . increases substantially to being very difficult and costly to deploy." In short, this punch list item neither meets an assistance requirement contained in Section 103 nor is a cost-effective method of communicating required information to law enforcement, contrary to Section 107(b)(1), and, ultimately, Section 107(b)(3).

A requirement that a wireless carrier generate notification messages to law enforcement for every network event involving a call would clearly have a major deterrent effect on carriers' willingness to invest in new technologies and services, because the messaging overhead associated with any advanced service would make such services economically unattractive. Accordingly, this requirement also violates Section 107(b)(4).

---

[40] The punch list items imply a premise that all of the transmissions over a carrier's network can be classified as either call content or call-identifying information. In fact, certain network messages, such as those associated with the management and operation of a cellular network, should be considered neither.

E. Timing Information

The Commission has tentatively proposed requiring compliance with a punch list item that would require time-stamping of all call-identifying messages associated with intercepts, and transmission of such messages within a specified time, where both content and call-identifying information are authorized. The Commission notes that the FBI has proposed that time stamps be accurate within 100 milliseconds and that the messages be delivered within 3 seconds of the beginning of the event.[41] AirTouch is strongly opposed to any such requirement.

This punch list item again demonstrates that the FBI is attempting to dictate CMRS carriers' system design and configuration, in direct violation of Section 103(b)(1)(A). Wireless networks involve the interaction of huge numbers of components at a wide number of locations, including not only the switching center but numerous cell sites (in some cases, hundreds of them), as well as the subscriber's handset. These extensive networks currently operate without any need for accurate, synchronized time clocks at every location where a network message might be generated. Implementation of this time-stamp proposal would effectively require that wireless carriers redesign virtually all of their facilities to ensure that there is access to a synchronized time clock at all locations, so that a 100-millisecond-accurate time stamp can be generated at the occurrence of every event that might potentially be subject to reporting as call-identifying information. This, in turn, would include virtually everything that happens in a cellular system, if the constant out-of-band signaling that causes the system to operate is potentially reportable as call-identifying information as a different punch list item proposes. Moreover, the accuracy of such time stamps would be difficult to maintain, given the many potential sources of delay as an event propagates through the system.

---

[41] *FNPRM* at ¶¶ 104-05.

One of AirTouch's vendors believes that it is capable of generating such time stamps and delivering them within three seconds with a high probability of success. Another vendor, however, asserts its inability to "timestamp . . . call identifying messages . . . with an accuracy of 100 milliseconds of the event." The same vendor believes it is very likely to be able both to time stamp within five seconds and deliver the message within three seconds — a capability that it plans to deliver upon implementation of J-STD-025. Increasing accuracy and speed beyond that level, it claims, will "increase the cost of implementation exponentially with decreasing time." In sum, it is questionable whether the highly accurate, rapidly delivered time stamp would be a cost-effective method of achieving anything.

AirTouch submits, moreover, that such a time stamp does not constitute call-identifying information, as the Commission claims, and is therefore not subject to a Section 103 assistance requirement. The Commission asserts that the proposed time stamp is call-identifying information because it facilitates identification of the call-identification information with the call, and also because it facilitates compliance with Section 103(a)(2). AirTouch disagrees with this contention. The time stamp is not part of the call, does not identify the "origin, direction, destination, or termination" of the call, and would not have been picked up from the call on a traditional pen-register or trap-and-trace interception. Accordingly, it does not meet the statutory definition of call-identifying information, much less a cost-effective method of providing it, contrary to Section 107(b)(1); as a result it would also, ultimately, raise costs to residential consumers, in violation of Section 107(b)(3).

Moreover, time stamped call-identification information of specified accuracy and promptness is not necessary for compliance with Section 103(a)(2). That section simply requires the delivery of call-identifying information "before, during, or immediately after" a communication, "or at such later time as may be acceptable to the government," and "[i]n a manner that allows it to be associated

with the communication to which it pertains." It does not require transmission of call-identifying information immediately after each event reported, but is fully satisfied if all of the call-identifying information is transmitted "immediately after" the communication has terminated. Given the need to interpret Section 103's requirements narrowly, the Commission cannot lawfully impose a requirement that transforms those requirements entirely and requires different information to be reported at a different time.

As was discussed previously, any requirement to generate call-identifying information messages for out-of-band signaling events that occur in the network concerning a call would tend to discourage the implementation of new services and technologies. If each such message must also bear a time stamp and be delivered within some specified period of the event, the disincentive becomes even greater. Accordingly, the time stamp punch list item would contravene Section 107(b)(4).

F. Surveillance Status

The *FNPRM* tentatively concludes that the FBI's surveillance status message punch-list item is not an assistance capability under Section 103.[42] AirTouch agrees. This is a message that conveys neither call content nor call identifying information. Instead, it conveys information about the readiness of any number of systems in the wireless carrier's plant when there is no call under surveillance.

The cost and complexity of such a requirement is considerable, given the number of systems that would have to be monitored and audited on a periodic (or even constant) basis. Even the carrier's billing system might need to be checked, to determine whether an intercept will be affected by a denial of service for nonpayment. One vendor informed AirTouch that because of the potential

---

[42] *FNPRM* at ¶¶ 109-110.

scope of the systems that might have to be audited periodically, "implementation of this punch list item would be extremely costly." As a result, this would not be cost-effective, in violation of Section 107(a)(1) and would adversely affect residential subscriber rates, contrary to Section 107(a)(3). Moreover, this requirement would tend to discourage carriers from deploying new services and technologies, because of the cost of periodically auditing them, in violation of Section 107(a)(4).

G. Continuity Check Tone

The *FNPRM* also correctly concludes, albeit tentatively, that the FBI punch list proposal to require a continuity check tone "is not necessary to meet the mandates of Section 103(a)."[43] AirTouch agrees that this feature is not required by CALEA and may not, therefore, be required for compliance with the safe harbor requirements. AirTouch does note that if law enforcement agencies wish to pay for a continuity test tone, carriers with the capability of providing it will likely be willing to do so, since it appears to be feasible and poses no threat to privacy or security of communications.

H. Feature Status

The Commission also correctly concludes that the feature status messages sought by the FBI do not fall within the scope of Section 103(a).[44] Indeed, the Commission's explanation — that they do not constitute call-identifying information because they "do not pertain to the actual placement or receipt of individual calls'"[45] — is equally applicable to several other punch list items that the Commission nevertheless proposed to require, such as subject-initiated dialing and signaling information.

---

43 *FNPRM* at ¶ 114.

44 *Id.* at ¶ 121.

45 *Id.*

Implementing this feature "would be of moderate difficulty," according to one vendor. It could be implemented either by periodically auditing the feature systems or by modifying the feature systems to generate a message whenever there is a change. The cost, of course, would depend on which method were required for implementation (assuming it fell within the scope of Section 103(a)). Given that this item does not meet any requirements of Section 103, however, requiring it would violate Section 107(b)(1).

I. Dialed Digit Extraction

Finally, the Commission tentatively proposes to require compliance with the FBI's punch list concerning post-cut-through dialed digit extraction, as call-identifying information.[46] The rationale for this requirement is that such post-cut-through digits may be used for the routing of a call through another carrier's facilities.

AirTouch strongly objects to this proposal. Cellular and PCS systems do not use DTMF audio digits for their call routing, as landline networks do. Instead, they utilize pro-origination dialing, with the digits transmitted out-of-band prior to voice channel setup. Accordingly, any DTMF digits transmitted over a cellular or PCS system do not constitute "dialing or signaling information that identifies the origin, direction, destination, or termination" of the communication provided by the cellular or PCS carrier. As a result, they do not constitute call-identifying information. On such a system, all DTMF digits dialed will be post-cut-through, will not be interpreted or acted upon by the wireless carrier for purposes of call routing, and constitute call content. They are interpreted, if at all, only by the recipient of the call. Congress specifically distinguished post-cut-through digits from those used for "routing calls through the telecommunications carrier's network," stating that "[o]ther dialing tones that may be generated by the sender that

---

[46] *FNPRM* at ¶ 128.

are used to signal customer premises equipment of the recipient *are not to be treated as call-identifying information.*"[47]

Cellular and PCS carriers do not currently have any reason even to detect such tones, unlike landline telephone carriers. Accordingly, they have no way to know what purpose is served by a customer's post-cut-through DTMF digits. Such digits may be used to provide a called number to an interexchange carrier or operator service provider, they may be used to navigate an automated attendant or voice mail system, or they may be used to enter a credit card number into an information service provider's computer. To the wireless carrier, they are simply call content.

To the extent that a law enforcement agency has a Title III intercept authorization, it will receive the DTMF digits over its call content channel like any other content. Without a Title III intercept authorization, however, the cellular or PCS carrier is simply unable to distinguish those digits used for call routing from those used for transmission of information. If a law enforcement agency has only been authorized to obtain call-identifying information, the wireless carrier will be unable to provide only the digits dialed for call routing.

AirTouch has been advised by multiple vendors that it would be possible to extract dialed digits post-cut-through, but none of its vendors claim to be able to reliably distinguish digits used for call routing in a subsequent leg of the call from digits used solely for the transmission of information. As one vendor put it, "no solution based on extracting the digits . . . could distinguish between call-identifying digits and digits dialed to performed other functions." Accordingly, either all of the digits must be denied to law enforcement, or all of them must be turned over — assuming the carrier is obligated to extract and decode the digits in the first place.

---

[47] House Report at 21 (emphasis added).

The cost of extracting and decoding the DTMF digits would be substantial because hardware as well as software would be required. One vendor notes that this requirement would require that tone capture and decoding equipment "be allocated for every call involving a target," and the other vendors agree. Another vendor notes that such hardware "would have to be provisioned for CALEA, only . . . [and] could not be shared with any other switching function." One vendor estimates that each dialed digit extraction unit would cost about $1000. Thus, a system with a capability of conducting 200 simultaneous wiretaps (including multiple legs of conference calls, if required) would need to have 200 such units, costing roughly $200,000, an amount comparable to the per-switch cost of the software upgrade for the entire punch list. One vendor concluded that implementation of this punch list item would require "major software re-architecture" and "significant changes . . . to the engineering and capacity"of the switching office to accommodate the hardware, concluding "that the Dialed Digit Extraction feature is cost prohibitive."

Given that the digits are already available for interception by law enforcement on a call content channel, provided a Title III intercept has been authorized, the hardware and software costs associated with dialed digit extraction are clearly not a cost-effective manner of providing these digits to law enforcement. Accordingly, this punch list item is precluded by Section 107(b)(1) and (3). Moreover, the Commission's proposal to treat the dialed digits as call-identifying information would clearly violate the minimization requirement of Section 107(b)(2), since it would not be possible to screen out digits that constitute solely call content.

J. Time Required for Compliance with the Punch List

After consultation with all of its vendors, it is clear to AirTouch that considerable time is needed before compliance with the punch list can reasonably be required. First, it is essential that the Commission provide considerable clarification concerning what is and is not required, which may take further proceedings. Second, after the Commission finalizes the overall requirements, it

will be necessary to conduct further industry standards-setting procedures. Upgrades can proceed only many months after the *final adoption of standards.* This is critical: Manufacturers cannot make major commitments of time and resources to development of software or hardware upgrades before the detailed standards have been finalized. Accordingly, if additional requirements are imposed on the industry by the FCC, manufacturers cannot simply proceed to develop upgrades, because the industry standard-making process must be completed first. Vendors have advised the Commission (and FBI) of this critical fact.

One of AirTouch's vendors estimated that *if* the Commission were to issue a decision by the second quarter of 1999, and *if* the decision did not introduce a great deal that deviates from the standards work that is already underway, it might be possible to move the standards process to a ballot by the end of 1999. Adding an estimated 18 to 24 months for product development and an additional 9 months for widespread deployment results in an implementation *target* in late 2002 — as the earliest date for compliance that can reasonably be expected.

III. THE INDUSTRY-DEVELOPED STANDARD, J-STD-025, REASONABLY ASSURES COMPLIANCE WITH THE CALEA ASSISTANCE CAPABILITY REQUIREMENTS

Congress expressly relied on industry standard-setting efforts as the preferred way for carriers and manufacturers to come into compliance with CALEA's assistance capability requirements. Instead of granting the Commission broad rulemaking authority to implement the statute, Congress adopted the "safe harbor" provision, Section 107(a), which ensures that compliance with "public available technical requirements or standards adopted by an industry association or standard-setting organization" will cause a carrier or manufacturer to be found in compliance with the Section 103 requirements.[48] Such industry-developed requirements carry a strong presumption of validity and

---

[48] CALEA § 107(a)(2), 47 U.S.C. § 1006(a)(2); *see* House Report at 26.

are not to be set aside or supplanted by the Commission lightly. Congress authorized the FCC to override, supplement, or supersede industry standards only in response to a petition showing them to be deficient (*i.e.*, the Commission may not engage in standards rulemaking on its own motion), and only if it meets the high burden established by the statutory criteria discussed in the preceding section — including that the Commission must show that its requirements are a cost-effective way to meet the assistance capability requirements of the statute.

The Commission has acknowledged that "industry is in the best position to determine how to implement [the] technical requirements [of Section 103(a)] most effectively and efficiently."[49] Under the safe harbor provision, a manufacturer's or carrier's compliance with the industry-adopted J-STD-025 will, by operation of law, cause such carrier or manufacturer to be found in compliance with Section 103, and that will continue to be the case unless and until the Commission propounds additional or changed requirements in accordance with the statutory standards.

AirTouch submits that the industry standard, which was developed after years of effort, with extensive input from law enforcement agencies, is a reasonable way of achieving compliance with the Section 103 assistance requirements and comports with the law. And as shown in the preceding section, the FBI's punch list items do not satisfy the statutory criteria for overriding this industry-established standard. In this section, AirTouch addresses issues concerning compliance with J-STD-025.

A. Implementation of J-STD-025 and Full Compliance by Providers Will Likely Require Additional Time, Due to Reliance on Vendors

First, AirTouch notes that the time currently allotted for compliance with the industry standard is likely to be insufficient for full national roll-out of CALEA-compliant hardware and

---

[49] *FNPRM* at ¶ 34.

software. Carriers are completely dependent on their vendors for the provision of hardware and software upgrades needed to comply with the standard. Some vendors may not be capable of supplying all of the needed upgrades and rendering them fully operational by the current June 30, 2000 deadline. While most of its vendors have informed AirTouch that they expect to have upgrades generally available in advance of the deadline, they also acknowledge that the nationwide "roll-out" of these upgrades — the delivery, installation, testing, and implementation of their capabilities — will not likely be fully achievable by the deadline.

Manufacturers have to respond to numerous demands in their product development cycles. Among the most important demands, of course, is the need to provide features and capabilities that benefit end users. In the competitive wireless industry, manufacturers are under constant pressure from carriers to respond to the demands of customers in the marketplace. In addition, manufacturers must deal with the Y2K issue and implement a variety of new technical requirements imposed by the Commission at the same time as they are working to ensure compliance with J-STD-025.

In addition, CALEA requires that manufacturers make CALEA-compliant hardware and software available on a "reasonably timely basis."[50] Vendors have indicated to AirTouch that in accordance with this requirement, they intend to incorporate CALEA compliance — including compliance with J-STD-025 and any subsequent requirements based on the punch list — into their products in accordance with their regular development and release cycles. Product development cycles generally are fixed well in advance, with (for example) an annual release of a software upgrade, for which development efforts begin only after completion of the previous annual software upgrade. Because of the fixed schedule for including items in an upgrade development cycle, manufacturers require a minimum lead time of 12 to 18 months, and in some cases even 24 to 36

---

[50] CALEA § 106(b), 47 U.S.C. § 1005(b).

months, from the final adoption of standards to the scheduled general availability of the upgrade incorporating the standards. Moreover, the deployment and installation of an upgrade requires many months of effort by both the vendor and the carrier after it reaches general availability. While some systems may be able to complete installation of an upgrade within six months of release, nationwide deployment may require a year or even longer.

AirTouch has contacted its vendors to attempt to determine whether they are fully prepared to have J-STD-025 compliance fully implemented by the existing June 30, 2000 deadline. One vendor informed AirTouch that it "expects" to finish providing AirTouch with core J-STD-025 features "during the first calendar quarter of 2000," but notes the possibility that unspecified "problems or delays" may occur. A second vendor stated that it plans its core J-STD-025 product to be "developed close to . . . December 1999" and that it expects to be able to have this upgrade fully installed and deployed in an AirTouch market by the June 2000 deadline, but that it does *not* believe six months is sufficient for deployment to all customers nationwide and estimates that an additional three months may be necessary. A third vendor affirmed that its core J-STD-025 upgrade "is currently scheduled for General Availability in December 1999." Subsequently, this vendor acknowledged that this upgrade depends on the timely and successful implementation of an earlier 1999 upgrade release, which will contain the "lion's share of the implementation." This vendor also acknowledged that the "roll-out process" will begin only after the upgrade is released and will take considerable time — the vendor maintains that it will be "tight" for AirTouch to be compliant by June 2000, asserting without qualification that "the entire network," *i.e.,* all of the vendor's systems nationwide, "won't be done by June 30, 2000."

Based on these indications, it is inevitable that the Commission will have to entertain justifiable requests for extension of the June 30, 2000 deadline. The Commission should acknowledge that additional extensions may be necessary in its *Report and Order* herein.

B. Location Information, as Interpreted by the Commission, Is Achievable

Three of the four vendors with which AirTouch communicated asserted specifically that their core J-STD-025 solutions include the location information the Commission has proposed to require — *i.e.,* the cell site locations at the beginning and end of a wireless call. All of the same caveats discussed in the foregoing section apply to these vendor projections — all of the vendors' assurances, estimates, and projections are "soft," in that there are innumerable potential sources of delay and other complications. Moreover, as discussed above, it is unlikely that the June 30, 2000 deadline will be achieved fully, even without major problems.

The vendors' J-STD-025 compliance projections are premised on the addition of no new requirements. Clearly, if the Commission ultimately requires more detailed location information than the cell sites handling a call at its beginning and end, additional work would have to be done, and the June 30, 2000 date cannot be met for this part of the standard. Moreover, adding to the scope of this item would pose problems under CALEA, in that Section 103 provides that "call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[51]

C. Packet-Mode Issues Should Be Deferred to a Further Rule-making

Two vendors supplied AirTouch with preliminary and incomplete information concerning their ability to design a solution for providing access to packet-mode communications. Both vendors expressed concern that there is little clarity concerning which communications need to be extracted from the packet stream and how this is to be accomplished. Both vendors stated that the J-STD-025 provides insufficient guidance to achieve technical compliance and that further standards work

---

[51] CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2).

would be required, once the objectives are more clearly stated. The development of an upgrade to provide packet-mode assistance would require the lead time discussed above (between 12 and 36 months) from adoption of a detailed standard, plus six months to a year for full deployment.

The vendors' consensus appears to be that it would be possible to provide access to the raw packet stream, but that identifying and extracting particular packets, or header information from those packets, from an otherwise random stream in real time would be difficult to impossible to accomplish, given the wide variety of protocols in use now, not to mention the use of additional protocols in the future. In light of the fact that a packet stream contains an intermixture of different, unrelated parties' communications, compliance with the requirement to safeguard the privacy and security of communications not authorized to be intercepted could not be achieved by providing law enforcement with access to the raw packet stream.

Accordingly, AirTouch submits that the Commission should exclude the provisions of J-STD-025 concerning packet mode communications, as proposed in the *FNPRM*.[52] Further proceedings are needed to determine how to treat the very difficult problems posed by the application of CALEA to packet-mode communications. After the policy issues have been thoroughly addressed by the Commission in a notice-and-comment rulemaking proceeding focused

---

[52] The packet-mode interception requirement clearly will affect future services, such as third-generation mobile voice/data/multimedia services and services built on a distributed packet-based architecture; it may also affect dedicated mobile data services not currently offered by AirTouch. With respect to currently offered cellular-based data services, such as CDPD, vendors' views diverge, based on the architecture employed. One vendor indicated to AirTouch that its architecture handles CDPD messages at the intercept point (*i.e.*, the switch) as circuit-switched communications, and such messages are thus capable of interception in accordance with J-STD-025 in the same manner as any other circuit-switched communication, in its implementation. Another vendor, however, has expressed the view that providing interception of call content and call identifying information for mobile-to-mobile CDPD traffic, under its system architecture, is "not reasonably achievable" and would require major architectural changes that "could be considered not cost effective" in light of the low level of mobile-to-mobile data traffic.

on the packet-mode issues, the development of standards achieving those policies should be remanded to industry standards bodies.

CONCLUSION

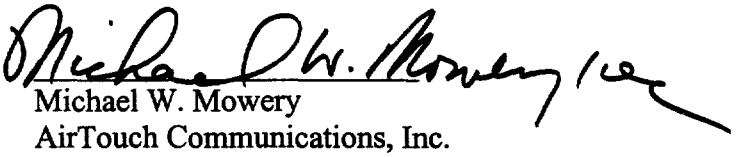
For the foregoing reasons, AirTouch respectfully supports the Commission's proposal to allow the core features of J-STD-025, including originating and terminating cell site locations, to become an effective safe harbor under CALEA. AirTouch opposes, however, the Commission's proposal to require compliance with any provisions of the FBI punch list. These items exceed the requirements of CALEA and should be rejected by the Commission.

Respectfully submitted,

AIRTOUCH COMMUNICATIONS, INC.

By: 

Pamela J. Riley
David G. Gross
AirTouch Communications, Inc.
1818 N Street, N.W., Suite 800
Washington, D.C. 20036
(202) 293-3800

By: 

Michael W. Mowery
AirTouch Communications, Inc.
2999 Oak Road, MS1025
Walnut Creek, CA 95596
(510) 210-3804

December 14, 1998

ATTACHMENT A

REPRESENTATIVE LETTER TO VENDORS

ATTACHMENT A

AIRTOUCH™
Cellular

Michael J. Polonsky
Executive Vice President
Network & Systems Operations

AirTouch Cellular
2999 Oak Road, MS 650
Walnut Creek, CA 94596

Telephone: 510 210 3939
Facsimile: 510 210 3636

November 17, 1998

Via Fax to: Mr. and
Certified Mail - Return Receipt Requested

Re: Request for Information Concerning FCC Proposed CALEA Standards

Dear

As you know, the Federal Communications Commission has issued a Notice of Proposed Rulemaking seeking comments by December 14, 1998 on standards for wireless carriers' implementation of the Communications Assistance for Law Enforcement Act ("CALEA").[1] AirTouch plans to file comments in response to the *NPRM*. We are, however, highly dependent upon our major equipment vendors in formulating our response.[2] Accordingly, we formally seek your assistance in providing the facts needed to respond to the *NPRM*.[3]

In the interest of preparing responsive comments on December 14, 1998, we need your immediate and continuing assistance. We therefore ask that you contact us upon receipt of this letter and that you provide us with a written response on or before December 3, 1998, to give AirTouch adequate time to prepare its comments.

---

1 Communications Assistance for Law Enforcement Act, CC Docket 97-213, *Further Notice of Proposed Rulemaking*, FCC 98-282 (Nov. 5, 1998) (*NPRM*).

2 Congress has recognized the "critical role" manufacturers will play in CALEA implementation, because "[w]ithout their assistance, telecommunications carriers likely could not comply with the capability requirements." H.R. Rep. No. 103-827, at 26 (1994).

3 We are making this request in fulfillment of our obligation under Section 106(a) of CALEA to consult with the manufacturers on whom we rely, *see* 47 U.S.C. § 1005(a), and your provision of support would be in keeping with the spirit of Section 106(b) of CALEA, 47 U.S.C. § 1005(b), which requires manufacturers to make available to carriers the features needed to comply with CALEA.

In the *NPRM,* the FCC approved the "core features" of the industry-developed standard, J-STD-025,[4] as satisfying the "safe harbor" provisions of Section 107(a) of CALEA, 47 U.S.C. § 1006(a). In so ruling, the Commission included as "safe harbor" requirements all of the uncontested parts of J-STD-025 and also proposed including the contested "location information" element, which the Commission has construed as requiring "cell site location at the beginning and termination of a call."[5] The only element of the J-STD-025 standard that the Commission has not proposed including as a "safe harbor" requirement is the provision of access to packet-switched communications.[6]

In order to take advantage of the "safe harbor" provisions by June 30, 2000, when CALEA compliance is currently scheduled to be mandatory, AirTouch needs to determine that it will be able to comply with all parts of the existing J-STD-025, with the possible exception of the packet-switched provisions, by that date. For that reason, we request that you confirm your ability to deliver the "core elements" of J-STD-025, including location information, in a cost-effective manner by the required date. The *NPRM* also sought comment on the possible inclusion of (perhaps modified or clarified) packet-switched provisions. Accordingly, we request that you explain your understanding of the technical details of the packet-switched provisions and the challenges posed thereby, and provide us with your input on whether this capability can be provided in a timely and cost-effective basis.

In addition, in the *NPRM,* the FCC addressed the deficiency petition filed by Department of Justice and FBI. It has proposed adoption of five provisions from the "punch list" submitted in this petition:

(1) **Content of subject-initiated conference calls;**
(2) **Identification of party hold, join, and drop on conference calls;**
(3) **Subject-initiated dialing and signaling information;**
(4) **Timing information**; and
(5) **Post-cut-through dialed digit extraction.**

The *NPRM* tentatively concluded that three "punch list" items should not be required — (a) **Surveillance status,** (b) **Continuity test tone**, and (c) **Feature status.** Finally, the Commission remained neutral in the *NPRM* regarding one "punch list" item, **In-band and out-of-band signaling.**

---

[4] *See* Telecommunications Industry Association and Electronic Industries Association, *Lawfully Authorized Electronic Surveillance,* Interim/Trial-Use Standards, J-STD-025 (December 1997).

[5] *NPRM* at ¶ 55.

[6] *See NPRM* at ¶ 46.

For each of the "punch list" items, we request that you provide us with information that will aid us in preparing comments addressed to each of the statutory standards for evaluating standards contained in Section 107(b) of CALEA — *i.e.*, whether a particular feature can be provided "by cost effective methods," while "protect[ing] the privacy and security of communications not authorized to be intercepted" and "minimiz[ing] the cost of such compliance on residential ratepayers," consistent with "encourag[ing] the provision of new technologies and services," and in "a reasonable time . . . for compliance." 47 U.S.C. § 1006(b). In addition, given that AirTouch is likely to be required to comply with the five "punch list" items that the FCC has proposed adopting, we ask that you confirm that your company can develop and provide each of these capabilities to AirTouch by June 30, 2000, or such other date as the FCC may establish.[7]

AirTouch needs *detailed* information in order to file comments that are responsive. The FCC emphasized in the *NPRM* that in evaluating the "punch list" items against the Section 107(b) standards, it is soliciting "information that is as detailed and specific as possible," including details concerning the costs to manufacturers and carriers, and how those costs will affect residential ratepayers. Moreover, the Commission asked commenters to "be specific as to what costs would be incurred for hardware, as opposed to software upgrades to carriers' networks, and whether some of these upgrades would have other uses in the networks."[8] Likewise, the Commission sought "detailed information" concerning technical requirements, including projected timelines.[9] To the extent that capacity requirements will affect your ability to provide solutions, we request that you provide information to us on how capacity will affect availability and cost, and indicate the capacity you have presumed in proposing your solutions.

In this connection, it is our understanding that a number of manufacturers have previously supplied cost and/or feasibility information concerning the "punch list" items to the FBI. If you have supplied such information, we ask that you provide copies to AirTouch, as well, so that we might have available to us information that will undoubtedly be used by the FBI and Department of Justice in their attempts to persuade the FCC to include "punch list" items in the capabilities standard.

---

7 *See NPRM* at ¶ 133.

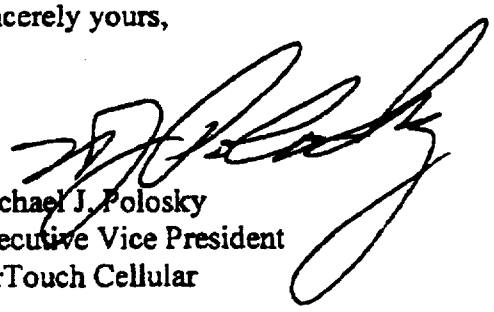
8 *Id.* at ¶ 30.

9 *Id.*

The FCC's CALEA implementation proceeding poses rare challenges to wireless telecommunications carriers and manufacturers. Given the schedule for the rulemaking, it is critical that you provide us with information as soon as possible to assist AirTouch in preparing its comments. In order to facilitate the necessary information-gathering, we recommend that your company designate a representative with whom AirTouch can work to begin to obtain the information it needs to prepare its comments.

Finally we recognize that some of the data we are requesting may be competitively sensitive. Accordingly, AirTouch commits to work with you before using any of your data in public comments to see that your interests are appropriately safeguarded. If you deem it necessary, we would be willing to execute a nondisclosure agreement that permits use of your data only in agreed-upon ways.

Sincerely yours,



Michael J. Polosky
Executive Vice President
AirTouch Cellular

cc: